WEB-BASED METHOD, APPARATUS, AND SYSTEM FOR SECURE DATA STORAGE

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of applicant's co-pending U.S. Application No. 09/536,203 filed March 27, 2000, the contents of which is hereby incorporated by reference.

FIELD OF THE INVENTION

This invention relates generally to the field of secure electronic data storage, and more specifically to a web-based, password controlled software system for encryption and decryption of data for secure data transmission and storage.

BACKGROUND OF THE INVENTION

Today, most computers are linked to other computer systems via a computer network. A computer network is basically a collection of computers that are physically and logically connected together to exchange data or "information." The network may be local area network (LAN), in which computers are geographically close together and connected by short segments of ethernet or to the same network hub, or wide area network (WAN), in which computers are separated by a considerable distance and are connected by telephone lines or radio waves. Often, networks are configured as "client/server" networks, such that each computer on the network is either a "client" or a "server." Servers are computers or processes dedicated to managing shared resources, such as

storage of electronic data. Any computer that performs a task at the command of another computer is a server.

An internetwork is a network of computer networks, of which the Internet is commonly acknowledged as the largest. The Internet is based on standard protocols that allow computers to communicate with each other even if using different software vendors, thus allowing anyone with a computer easy accessability to everything else connected to the Internet world wide. As a result of this global access, it is becoming increasingly useful for businesses and individuals to transmit information via networks and internetworks from one site to another.

The interconnected computers exchange information using various services, for example, the World Wide Web (WWW)and electronic mail. The HTML documents and other files related to a web generally reside on a web computer known as a web server. Although web servers vary greatly in processing speed and memory, they are essentially generic computers with a CPU, co-processors and memory. The different types of computers which can act as a server are well-known to those in the computer field.

The WWW is an application which allows users seeking information on the Internet to switch from server to server. The WWW service allows a server computer system (Web server or Web site) to send graphical Web pages of information to a remote client computer system. A program known as a web browser running on a client computer allows the client computer to communicate with the WWW. The remote client computer system can then display the Web pages.

Organizations are increasingly utilizing these networks to improve customer service

and streamline business communication through applications such as e-mail, messaging, remote access, intranet based applications, on-line support and supply chain applications. The very openness and accessibility that has stimulated the use of public and private networks has also driven the need for network security.

As the number of users to the Internet grows, so have concerns regarding the security of businesses and organizations which utilize the Internet for the transfer of confidential information. Security issues have become of increasing concern, particularly when connecting a network, such as a LAN, to the Internet. Such a connection can provide intruders with an opportunity to gain access to the a network.

A common method for preventing intrusion is allow only a secure single attachment point to the Internet. This method of defense is commonly referred to as a "fire wall." The single point of attachment allows the passage of only certain types traffic. This procedure can provide a relatively high level of security for a single user, however, maintain this security level becomes difficult as the number of users requiring Internet access increases.

One method of securing electronic data is to utilize encryption algorithms. Encryption algorithms transform written words and other kinds of messages so that they are unintelligible to unauthorized recipients. An authorized recipient can then transform the words or messages back into a message that is perfectly understandable. Currently, there are two basic kinds of encryption algorithms (1) symmetric key algorithms and (2) public key algorithms.

Symmetric (or private) key algorithms use the same key to encrypt and decrypt the

message. Generally, they are faster and easier to implement than public keys. However, for two parties to securely exchange information, those parties must first securely exchange an encryption key. Examples of symmetric key algorithms include DES, DESX, Triple-DES, Blowfish, IDEA, RC2, RC4, and RC5.

Public key algorithms use one key (public key) to encrypt the message and another key (private key) to encrypt it. The public key is made public and is used by the sender to encrypt a message sent to the owner of the public key then the message can only be decrypted by the person with the private key. Unfortunately, public keys are very slow, require authentication, and do not work well with large files.

A third type of system is a hybrid of the public and private systems. The slower public key cryptography is used to exchange a random session key, which is then used as the basis of a symmetric (private) key algorithm. The session key is used only for a single encryption session and is then discarded. Nearly all practical public key cryptography implementations in use today are actually hybrid systems.

Finally, message digest functions are used in conjunction with public key cryptography. A message digest function generates a unique pattern of bits for a given input. The digest distills the information contained in a file into a single large number, typically 128 and 256 bits in length. The digest value is computed in such a way that finding an input that will exactly generate a given digest is computationally infeasible.

Message digest algorithms are not used for encryption or decryption but for creation of digital signatures, messages authentication codes (MAC), and the creation of encryption keys from passphrases. For example, Pretty Good Privacy (PGP) uses message digests to

transform a passphrase provided by a user in to an encryption key that is used for symmetric encryption. (PGP uses symmetric encryption for its "conventional encryption" function as well as to encrypt the user's private key). A few digest in use are HMAC, MD2, MD4, MD5, SHA, and SHA-1.

Working cryptographic systems can be divided into two categories; (1) programs and protocols that are used for encryption of e-mail messages such as PGP and S/MIME and (2) cryptographic systems used for providing confidentiality, authentication, integrity, and nonrepudiation in a network environment. The latter requires real-time interplay between a client and a server to work properly. Examples include Secure Socket Layer (SSL) a general-purpose cryptographic protocol that can be used with any TCP/IP service and PCT a transport layer security protocol for use with TCP/IP service, PCT, S-HTTP, SET, Cybercash, DNSSEC, Ipsec, IPv6, Kerberos, and SSH.

Although the present means of securing electronic information provides a level of security, the security provided can be easily breached. Symmetric encryption algorithms are vulnerable to attack by (1) key search or brute force attacks, (2) cryptanalysis, and (3) systems-based attacks. First, in a key search, the cracker simply tries every possible key, one after another, until the he/she is allowed into the system or the ciphertext is decrypted. There is no way to defend against this but a 128 bit key is highly resistant because of the large number of possible keys to be tried.

Second, in cryptanalysis, the algorithm can be defeated by using a combination of sophisticated mathematics and computer power. Many encrypted messages can be deciphered without knowing the key. Finally, the cryptographic system itself is attacked

without actually attacking the algorithm. Public key algorithms are theoretically easier to attack then symmetric key algorithms because the attacker has a copy of the public key that was used to encrypt the message. Also, the message presumable identifies which public key encryption algorithm was used to encrypt the message. These attacks are (1) factoring attacks and (2) algorithmic attacks. First, factoring attacks attempt to derive a private key from its corresponding public key. This attack can be performed by factoring a number that is associated with the public key.

Second, an algorithm attack consists of finding a fundamental flaw or weakness in the mathematical problem on which the encryption system is based. Although not often done, it has been accomplished.

Message digest functions can be attacked by (1) finding two messages-any two messages-that have the same message digest and (2) given a particular message, find a second message that has the same message digest code.

It would be advantageous to provide a system for securing a server from outside intrusion, not by standard "firewall" barrier systems, but by encrypting the data residing on the server itself so as to render the data useless to a would-be intruder. It would also be desirable to implement such a system using a Web-based software application which can be used for both secure file storage and secure transmission of data.

SUMMARY OF THE INVENTION

The present invention provides a Web-based software system which is designed to administrate access and facilitate virtually impregnable security for the delivery, storage, and sharing of documents and files.

The invention includes a method of storing secure electronic data on an archive server, which comprises the steps of providing a plurality of client workstations running web browsers programs, accessing the WWW from a client workstation and logging onto a qualified web server, providing account qualifier data to a software application residing on the web server, downloading an encryption applet from the software application, selecting an electronic data file to be encrypted, encrypting the electronic data file and forming an encrypted data packet, storing the encrypted data packet on an archive server; and destroying said encryption applet.

The invention includes a method of retrieving encrypted electronic data stored on an archive server, comprising the steps of providing at least one encrypted data packet on an archive server, providing at least one client workstation having running a web browser program; accessing the web browser and logging onto a qualified web server; providing account qualifier data to a software application residing on the web server; selecting an encrypted data packet to be retrieved; downloading a decryption applet from the application based on the original encryption algorithm; transferring the decryption applet and the encrypted data packet to the client workstation; and decrypting the encrypted data packet at the client workstation, whereby readable electronic data is available to a user at the client workstation. If the encrypted data packet is compressed, the decryption applet

can include a decompression program to decompress the encrypted data packet.

At least two of the plurality of client workstations can be coupled via a network, such as a LAN or WAN. The archive server can be coupled to client workstations, or alternatively, can be accessed from the client workstation via the Internet using SSL protocol. The method can also include the step of compressing the encrypted data packet prior to transmission, and the encryption applet can include a compression program to compress the electronic data. The software application compiles the encryption applet using an encryption algorithm, and the encryption algorithm is preferably changeable with respect to the software application.

The method of the invention further includes the steps of providing a plurality of encryption algorithms which can be selected according to the needs of the user, selecting an encryption algorithm; and compiling the encryption applet to use the selected encryption algorithm.

The method can further includes the step of assigning access permission to said encrypted data packet, wherein the access permission permits selective access to the electronic data files. Access permission can be assigned to a user having designated account qualifier data. The access permission can also permits hierarchal access to an electronic data file by a group of users.

The invention includes a system for secure storage of electronic data on an archive server, which comprises a plurality of client workstations having web browsers running thereon. a platform-independent software application residing on an web server, means for qualifying a authorization user of the software application; and a means for encrypting an electronic file at said client workstations. The means comprises an encryption applet

compiled by the software application which is operable to encrypt the electronic file to create an encrypted data packet. In the system of the invention, the encryption applet is downloaded by a user at one of the client workstations. The system further includes a means for transmitting the encrypted data packet to the archive server for secure storage, a means for retrieving said encrypted data packet from said archive server; and means for decrypting the encrypted data packet, which comprises obtaining a decryption applet from said software application. The decryption applet compiled by said software application is based on the original encryption algorithm.

Accordingly, it is an objective of the instant invention provide a system, method and apparatus which secures electronic data residing on a network server by storing encrypted data on the server.

It is another objective of the invention to provide a system, method and apparatus for secure data storage which utilizes a Web-based software application accessed via a web browser running on a client workstation, thus obviating the need for client-side software.

It is still another objective of the instant invention to provide a system for secure storage of electronic data which uses a web-based software application residing on a web server, and stores encrypted electronic data on a local server.

It is a further objective of the instant invention to provide a method and apparatus that provides secure electronic transfer and storage of information by using a random and automatic mode of encryption wherein no two keys are ever repeated.

Still another objective of the instant invention to provide a method and apparatus that allows for secure data transportation and storage that encrypts at the 128 bit level,

transports and stores data encrypted, and decrypted only to an authorized user.

A further objective of the instant invention to provide a basic level of security wherein data is transported via an SSL protocol and automatically encrypted. In this mode only authorized user on a network can access data for review or modification.

Another objective of the instant invention to provide a heightened level of security wherein a private and secondary key or digital file lock can be employed providing a unique secondary data lock.

A still further object of the instant invention is to provide a web-based security system which permits universal, remote access by client workstations to data residing on an archive server.

Still another objective of the instant invention to provide a client-side locking device or biometric interface. In such a locking device, a retinal scanner, finger print scanner, smart card reader or the like can be utilized to send or retrieve information.

Yet another objective of the instant invention is to provide virtually impregnable security for the delivery, storage, and sharing of documents and files utilizing any compatible network as a secure communications forum.

Other objects and advantages of this invention will become apparent from the following description taken in conjunction with the accompanying drawings wherein are set forth, by way of illustration and example, certain embodiments of this invention. The drawings constitute a part of this specification and include exemplary embodiments of the present invention and illustrate various objects and features thereof.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is a block diagram of the steps executed by a software application for encryption and decryption of electronic data for secure data storage according to the instant invention;

Figure 2 is a block diagram of the account authorization process according to a preferred embodiment of the instant invention;

Figure 3 is a block diagram of the encryption and storage of electronic data as represented by step A in Fig. 1;

Figure 4 is a block diagram of the retrieval and decryption of electronic data as represented by step B in Fig. 1;

Figure 5 is a diagram illustrating a hierarchal access structure for different user groups;

Figure 6 is a schematic illustration of a first system according to a preferred embodiment of the invention using client workstations coupled via a network;

Figure 7 is a schematic illustration of a second system according to a preferred embodiment of the invention using standalone client workstations which are not networked to one another; and

Figure 8 is a schematic illustration of a third system according to the preferred embodiment of the invention using a standalone personal computer.

DETAILED DESCRIPTION OF THE INVENTION

Although the invention will be described in terms of a specific embodiment, it will be readily apparent to those skilled in this art that various modifications, rearrangements, and substitutions can be made without departing from the spirit of the invention. The scope of the invention is defined by the claims appended hereto.

Now, referring to Fig. 1, shown is flow chart depicting the steps 100 executed by a Web-based software application 100 for encrypting data to be stored and decrypting data to be retrieved. In step 101, a user at a client workstation opens a web browser and accesses a qualified web server. The data transfer request is initiated in step 103. In step 105, account qualifier data is entered by the user, and the account qualifier data is authenticated by the server (shown in detail as steps 200 in Fig. 2). If the data cannot be authenticated, the transfer request is refused in step 109. If the account qualifier is authenticated, the user at the client workstation can encrypt a file and store it on an archive server 111, or retrieve the file from the archive server and decrypt the file 113.

A preferred method 200 of authenticating account qualifier data is shown in Fig. 2. In addition to the method 200, the invention contemplates a variety of methods to authenticate account qualifier data, and the invention is not limited in this regard. The server 12 provides login account qualifier data requiring either user name and a password 14 or a biometric interface 16 such as a retinal scanner, finger print scanner, smart card reader and the like for the purpose of seeking data-base authentication 18. If login fails, the user has three attempts 20 before the account is locked 22 and the administrator and the account holder 24 is alerted. Upon a successful login 26, a transfer request 28 is sent to the

control program on the server to open a transfer information page inquiry page.

Referring now to Figure 3, when data is to be transferred 30, an applet is compiled on the server and sent to the client workstation 32. The applet is a temporary file allowing the client to select 34 the data files that are to be transferred. The user adds the file(s) to be transferred to an application window 46. If the user account allows, the client has the option of entering via the keyboard, a secondary security key 36. It should be noted that even if two separate people encrypted the exact same file with the same key, they will have encrypted two uniquely different sequences. If one attempts to "crack" the application sequence, they would not be able to decrypt it because each applet is embedded with a unique encryption sequence. The encryption sequence generated is added to the applet template, and the data is encrypted and an encrypted data packet is compiled 38. The encrypted data packet is then transferred to the archive server 40. A notification 42 can be sent to an intended recipient of the file.

The applet breaks the code of the files down into its binary form during execution. It reads the binary data and then rewrites the data to the temporary file that was previously created. The running program changes the entire code sequence of the client file to a randomly generated sequence specified by the particular and customized applet. The sequence is also designed to replace every other matching bit of binary code with a unique string. Thus, with this method, an "a", for example, will never be represented twice in the same file structure. This is designed to deter the common method of cracking encrypted code by repeated or pattern data. On a binary level, the code is rewritten and saved for transfer in a file format only decodable by the recipient. The applet then sends the

encrypted data to the server via SSL protocol. Once the transfer is complete, the applet deletes any trace of the file encrypted. With the destruction of the applet, no two applications are ever the same because each application contains it's own encryption sequence that cannot be replicated.

The encrypted data packet resides on the server 12 waiting for an intended recipient to download and unlock it. This creates the ability to maintain completely encrypted and secure data archives. When file retrieval is requested by a recipient, the server then accesses the original record information of the sequence or algorithm that it originally gave to the applet that the server created to encrypt the file.

In order to maximize the effective rate at which the encrypted data can be transferred between the client workstations and the web server, the encrypted data can be compressed 44. Data compression is well-known in the art, any suitable compression technique can be used. A preferred data compression technique is commonly referred to as "traditional compression." In traditional compression, a compression program scans the data for patterns that occur more than once and assigns a "token" to replace each of these patterns. Another preferred compression technique is known as "delta compression," which can be used when encrypted data is transmitted to the archive server and an earlier verison of the encrypted data file is already on the archive server. A delta compressor sends only those portions of the file which is different than the earlier version of the file.

Now referring to Fig. 4, shown is the flow chart depicting the steps for decrypting data for a secure receipt of electronic data. If the login is successful, the server 12 depicts those files available to the recipient 66. The recipient chooses which file to retrieve and

the server generates a new applet designed to decrypt the encrypted data packet corresponding to the file requested 69, based on the original encryption sequence. The encrypted data packet is retrieved 70 and stored in a temporary file. The program now prompts the user for any secondary key 71 that was originally entered by the sender. Once the key sets the sequence, the applet calculates the sequence that was originally written on the fly. The applet resumes decryption with the new sequence of the temporary file wherein decryption is executed 72 and the decrypted file saved to a selection location. When the data decryption is complete, the program saves the file 73 with original extensions, to a folder specified by the recipient. Then the applet deletes itself 74 and any data related to the secure transfer. Upon completion of the transfer and decryption process, the original encrypted file located on the server can be triggered to be automatically deleted or retained for manual deletion.

Fig. 5 is a diagram of a first system according to a preferred embodiment of the present invention. A plurality of client workstations 111 are coupled via a LAN 114, or via any other computer network. The system includes a designated archive server 140 on which encrypted documents are stored in accordance with the method of the invention. Client workstations 111 can be any computer that is capable of providing access to the web server using a web browser, such as standard desktop computer systems, laptop computers, non-programmable terminals connected to a main frame, personal digital assistant, etc. The web browser running on the client workstations 111 is a software program that allows a user at the client workstations 111 to transmit and receive data over the Internet. A suitable web browser would be Internet Explorer 5.0.

A qualified web server 120 is linked to the WWW, and is accessed by client workstation 111 using a web browser. The software application 100 (Fig. 1) resides on qualified web server 120. In the preferred embodiment, software application 100 is a platform-independent application. Software application 100 is accessed by client workstation through an application gateway. Remote client workstations 112 can also have identical access to encrypted documents on archive server 140 by using a web browser 116 to access software application 100. Encrypted files can be transferred between the client workstations 111 and 112 and archive server 140 using SSL protocol on the WWW. An encrypted file can also be transmitted directly from client workstation 111 to archive server 140 via a secure local connection 142. In the preferred embodiment, varying levels of access to the encrypted files on archive server 160 is provided for the individual user so that access is "permission controlled."

The diagram in Fig. 7 illustrates another implementation of the system according to the invention. A plurality of client workstations 151 are linked to the WWW using the web browsers 156, and can access the software application 100 residing on qualified Internet server 120. Encrypted files are stored on and retrieved from archive server 160 in accordance with the method of the invention. The plurality of client workstations 151 are not coupled via a network, but rather have shared proprietary access to an archive server 160. This shared proprietary access is provided by the account qualifying function provided by software application 100. The plurality of client workstations 151 can therefore essentially comprise a "virtual" network.

An alternative arrangement using the system of the invention is illustrated in Fig. 8.

A personal computer 161 running a web browser 166 is linked to the WWW. The user can access software application 100 residing on qualified server 120. Files residing on the hard drive or other local media of personal computer 161 can be encrypted in accordance with the method of the invention using software application 130 in the manner herein described, and then archived on hard drive or other local media of personal computer 161. The system of the invention can thus provide document encryption security protection for an stand-alone workstation.

The invention can utilize any suitable encryption algorithm, such as Rijndael or Blowfish. The encryption algorithm is preferably "modular" with respect to the software application 100 in that the algorithm can be changed at any time, while still retaining the ability to decrypt older files which may be stored on the archive server. In another aspect of the invention, the user can select the encryption algorithm to be used depending on the user's security needs and the type of file to be encrypted. The selection of encryption algorithm can be session specific.

It is to be understood that while a certain form of the invention is illustrated, it is not to be limited to the specific form or arrangement of parts herein described and shown. It will be apparent to those skilled in the art that various changes may be made without departing from the scope of the invention and the invention is not to be considered limited to what is shown and described in the specification and drawings.